|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| id | \_id | str |
| index | \_index | str |
| score | \_score | int |
| source | \_source | json |
| type | \_type | str |
| version | \_version | int |
| fields | fields | json |
| timestamp | @timestamp | timestamp |
| version | @version | str |
| Geolocation IP Extension | geoip\_ext | json |
| host | host | str |
| path | path | str |
| T-Pot Hostname | t-pot\_hostname | str |
| T-Pot IP Extension | t-pot\_ip\_ext | str |
| T-Pot IP Interface | t-pot\_ip\_int | str |
| tags | tags | list |
| type | type | str |

Table 1 – Common parameters for all honeynets

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| timestamp | timestamp | timestamp |
| Event id | eventid | str |
| session | session | str |
| Source IP | src\_ip | str |
| duration | duration | str |
| Geolocation IP | geoip | json |
| IP Reputation | ip\_rep | str |
| sensor | sensor | str |

Table 2 – Parameters for Adbhoney

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| timestamp | timestamp | str |
| Destination IP | dest\_ip | str |
| Source IP | src\_ip | str |
| Geolocation IP | geoip | json |
| message | message | str |
| Printable Payload | payload\_printable | str |

Table 3 – Parameters for Ciscoasa

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source IP | src\_ip | str |
| Geolocation IP | geoip | json |
| Source Port | src\_port | int |
| File State | fileinfo.state | str |
| Destination Port | dest\_port | int |
| File Name | fileinfo.filename | str |
| Level | level | str |
| HTTP Method | http.http\_method | str |

Table 4 – Parameters for CitrixHoneypot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source IP | src\_ip | str |
| Geolocation IP | geoip | json |
| Source Port | src\_port | int |
| Data type | data\_type | str |
| Destination IP | dest\_ip | str |
| ID | id | str |
| Destination Port | dest\_port | int |
| timestamp | timestamp | str |
| Sensor ID | sensorid | str |
| Request | request | null |
| Event Type | event\_type | str |
| Public IP | public\_ip | str |
| Response | response | null |
| IP Reputation | ip\_rep | str |

Table 5 – Parameters for Conpot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source IP | src\_ip | str |
| Geolocation IP | geoip | json |
| Session | session | str |
| Message | message | str |
| Timestamp | timestamp | str |
| Duration | duration | float |
| Event ID | eventid | str |
| Sensor | sensor | str |
| IP Reputation | ip\_rep | str |

Table 6 – Parameters for Cowrie

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Session | session | str |
| ID | id | str |
| Level | level | str |
| Message | msg | str |

Table 7 – Parameters for Dicompot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Timestamp | timestamp | str |
| Connection | connection | json |
| Source Hostname | src\_hostname | str |
| IP Reputation | ip\_rep | str |

Table 8 – Parameters for Dionaea

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| HTTP User Agent | http\_user\_agent | str |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| HTTP URL | http.url | str |
| Event Type | event\_type | str |
| Timestamp | timestamp | str |
| Request Method | request\_method | str |
| Event ID | eventid | str |
| Sensor | sensor | str |
| IP Reputation | ip\_rep | str |

Table 9 – Parameters for ElasticPot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Timestamp | timestamp | str |
| FATT TLS | fatt\_tls | json |
| Protocol | protocol | str |

Table 10 – Parameters for Fatt

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Column 11 | column11 | null |
| Message | message | str |
| Username | username | null |
| Password | password | str |
| Authentication ID | auth\_id | str |
| Protocol | proto | str |
| Session ID | session\_id | str |

Table 11 – Parameters for Heralding

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Session | session | str |
| Request | request | str |
| Event Type | event\_type | str |
| Response | response | str |
| Sensor | sensor | str |
| IP Reputation | ip\_rep | str |

Table 12 – Parameters for Honeysap

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Is Virtual | is\_virtual | boolean |
| Proxy Connection | proxy\_connection | json |
| Downloads | downloads | json |
| End Time | end\_time | str |
| Operation Mode | operation\_mode | int |
| Attack Connection | attack\_connection | json |
| Start Time | start\_time | str |
| Download Tries | download\_tries | int |
| Download Count | download\_count | int |

Table 13 – Parameters for Honeytrap

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination Port | dest\_port | int |
| SMTP Input | smtp\_input | list |
| Timestamp | timestamp | timestamp |
| Data | data | str |

Table 14 – Parameters for Mailoney

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination Port | dest\_port | int |
| Destination IP | dest\_ip | str |
| Message | message | str |
| Level | level | str |
| Timestamp | timestamp | timestamp |
| Data | data | str |

Table 15 – Parameters for Medpot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination Port | dest\_port | int |
| Message | message | str |

Table 16 – Parameters for Rdpy

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Server Message Block (SMB) | smb | json |
| Flow ID | flow\_id | int |
| Incoming Interface | in\_iface | str |
| Timestamp | timestamp | timestamp |
| Protocol | proto | str |
| Event Type | event\_type | str |

Table 17 – Parameters for Suricata

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination Port | dest\_port | int |
| Status | status | int |
| Response Message | response\_msg | json |
| Peer | peer | json |
| Timestamp | timestamp | timestamp |
| Cookies | cookies | json |
| Method | method | str |
| UUID | uuid | str |
| Headers | headers | json |

Table 18 – Parameters for Tanner

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| HTTP User Agent | http\_user\_agent | str |
| Internet Printing Protocol (IPP) Query | ipp\_query | json |
| HTTP URL | http.url | str |
| Timestamp | timestamp | timestamp |
| Data | data | str |
| Event ID | eventid | str |
| Sensor | sensor | str |
| Request Method | request\_method | str |
| Headers | headers | json |
| IP Reputation | ip\_rep | str |

Table 19 – Parameters for Ipphoney

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| DNS Class | dns\_cls | str |
| Operation Code | opcode | int |
| DNS Type | dns\_type | str |
| DNS Name | dns\_name | str |
| IP Reputation | ip\_rep | str |
| Headers | headers | json |

Table 20 – Parameters for Ddospot

|  |  |  |
| --- | --- | --- |
| **Parameter** | **Field names in Collections** | **Schema** |
| Source Port | src\_port | int |
| Geolocation IP | geoip | json |
| Source IP | src\_ip | str |
| Destination IP | dest\_ip | str |
| Destination Port | dest\_port | int |
| Level | level | str |
| Action | action | str |
| IP Reputation | ip\_rep | str |
| Headers | headers | json |
| Message | msg | str |

Table 21 – Parameters for Redishoneypot